

What is claimed is:

1           1.       A system for providing Web-based remote security application  
2 client administration in a distributed computing environment, comprising:  
3           a self-extracting configuration file containing an executable configuration  
4 file that is self-extractable on a target client into an administered security  
5 application;  
6           an executable control embedded within an active administration Web  
7 page, the executable control being triggered upon each request for the active Web  
8 page and causing dynamic Web content to be generated therefrom;  
9           a Web server exporting a Web portal comprising the active administration  
10 Web page to a browser application independent of a specific operating  
11 environment and interpreting the executable control to facilitate copying of the  
12 self-extracting configuration file to the target client.

1           2.       A system according to Claim 1, further comprising:  
2           the Web server facilitating copying of the self-extracting configuration file  
3 concurrently to a plurality of target clients.

1           3.       A system according to Claim 1, further comprising:  
2           the Web server checking administrator credentials while exporting the  
3 Web portal against a list of authorized administrators.

1           4.       A system according to Claim 1, further comprising:  
2           the Web server monitoring the status of the copying of the self-extracting  
3 configuration file to at least one target client.

1           5.       A system according to Claim 1, further comprising:  
2           the Web server reporting the status of security application configuration  
3 on at least one target client.

1           6.       A system according to Claim 1, further comprising:

2 the self-extracting configuration file performing at least one of an  
3 installation, configuration, updating, and patching of the security application by  
4 executing the executable configuration file.

1 7. A system according to Claim 1, wherein the executable  
2 configuration file comprises at least one of a virus scanning, virus screening,  
3 active security, firewall, and VPN performance reporting application.

1 8. A system according to Claim 1, wherein the executable  
2 configuration file is a cabinet archival file.

1 9. A system according to Claim 1, wherein the active control is an  
2 Active X-compliant control.

1 10. A system according to Claim 1, wherein the distributed computing  
2 environment is TCP/IP-compliant.

1 11. A method for providing Web-based remote security application  
2 client administration in a distributed computing environment, comprising:  
3 storing a self-extracting configuration file containing an executable  
4 configuration file that is self-extractable on a target client into an administered  
5 security application;  
6 providing an executable control embedded within an active administration  
7 Web page, the executable control being triggered upon each request for the active  
8 Web page and causing dynamic Web content to be generated therefrom;  
9 exporting a Web portal comprising the active administration Web page to  
10 a browser application independent of a specific operating environment; and  
11 interpreting the executable control to facilitate copying of the self-  
12 extracting configuration file to the target client.

1 12. A method according to Claim 11, further comprising:  
2 facilitating copying of the self-extracting configuration file concurrently to  
3 a plurality of target clients.

1           13.     A method according to Claim 11, further comprising:  
2           checking administrator credentials while exporting the Web portal against  
3           a list of authorized administrators.

1           14.     A method according to Claim 11, further comprising:  
2           monitoring the status of the copying of the self-extracting configuration  
3           file to at least one target client.

1           15.     A method according to Claim 11, further comprising:  
2           reporting the status of security application configuration on at least one  
3           target client.

1           16.     A method according to Claim 11, further comprising:  
2           performing at least one of an installation, configuration, updating, and  
3           patching of the security application by executing the executable configuration file.

1           17.     A method according to Claim 11, wherein the executable  
2           configuration file comprises at least one of a virus scanning, virus screening,  
3           active security, firewall, and VPN performance reporting application.

1           18.     A method according to Claim 11, wherein the executable  
2           configuration file is a cabinet archival file.

1           19.     A method according to Claim 11, wherein the active control is an  
2           Active X-compliant control.

1           20.     A method according to Claim 11, wherein the distributed  
2           computing environment is TCP/IP-compliant.

1           21.     A computer-readable storage medium holding code for performing  
2           the method according to Claim 11.

1           22.     A system for remotely administering a client application using a  
2           Web-based portal in a TCP/IP-compliant environment, comprising:

3 an archival configuration file capable of self-extracting on a target client  
4 into an executable configuration file;

5 an executable control into an active administration Web page, the  
6 executable control being triggered upon each request for the active Web page and  
7 causing dynamic Web content to be generated therefrom;

8 a Web server serving the active administration Web page to a browser  
9 application to a requesting administrator, comprising:

10 a security module confirming credentials for the requesting  
11 administrator against a list of authorized administrators; and

12 a transfer module interpreting the executable control upon  
13 successful credentialing to facilitate substantially concurrent copying of the self-  
14 extracting configuration file to at least one target client.

1 23. A system according to Claim 22, further comprising:  
2 the Web server continuously monitoring the status of the copying of the  
3 self-extracting configuration file to the at least one target client; and  
4 the Web server generating a status event upon completion of the copying.

1 24. A system according to Claim 22, further comprising:  
2 the Web server reporting the status of each application configuration on  
3 the at least one target client.

1 25. A system according to Claim 22, wherein the active control is an  
2 Active X-compliant control.

1 26. A method for remotely administering a client application using a  
2 Web-based portal in a TCP/IP-compliant environment, comprising:  
3 storing an archival configuration file capable of self-extracting on a target  
4 client into an executable configuration file;  
5 embedding an executable control into an active administration Web page,  
6 the executable control being triggered upon each request for the active Web page  
7 and causing dynamic Web content to be generated therefrom;

8           serving the active administration Web page to a browser application to a  
9   requesting administrator, comprising:  
10           confirming credentials for the requesting administrator against a  
11   list of authorized administrators; and  
12           interpreting the executable control upon successful credentialing to  
13   facilitate substantially concurrent copying of the self-extracting configuration file  
14   to at least one target client.

1           27.    A method according to Claim 26, further comprising:  
2           continuously monitoring the status of the copying of the self-extracting  
3   configuration file to the at least one target client; and  
4           generating a status event upon completion of the copying.

1           28.    A method according to Claim 26, further comprising:  
2           reporting the status of each application configuration on the at least one  
3   target client.

1           29.    A method according to Claim 26, wherein the active control is an  
2   Active X-compliant control.

1           30.    A computer-readable storage medium holding code for performing  
2   the method according to Claim 26.